AMENDMENTS TO THE CLAIMS

Please amend claims 2 and 13.

Pursuant to 37 C.F.R. § 1.121 the following listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of the Claims:

Claim 1 (Canceled)

Claim 2 (Currently amended): A method for data storage on a server in a telecommunications network, the telecommunications network providing connectivity between local computers of users and the server, the method comprising:

issuing, upon request, by an operator of the server, to a first user of the users a user certificate for access conditions;

providing the user certificate and a secret key to the first user;

accessing the server over an internet;

sending, by the server, a client program to a first local computer of the first user, the client program enabling an authentication of the first user using the user certificate and a transmission of at least one further security requirement;

setting up a personal main folder on the server for the first user, the main folder having a first special file including a first security requirement defined for the main folder and first management information so as to provide a main locker;

configuring the personal main folder to have at least one further folder set up therein, the at least one further folder having a function and a second file including a second security requirement defined for the least one further folder and including second management information so as to provide a functional locker;

displaying the functional locker only if at least one security-relevant requirement is met so as to provide a locker system having a virtual character, wherein the functional locker provides ~~a function of at least one of:~~ a personal locker, wherein a reference to first files of the first user is storable in the personal locker only by the first user and displayable only to the first user, and at least one of:[[;]]

a provisioning locker, wherein a first reference to a different second file available to another user is storable therein only by the first user; and

a receiving locker, wherein a third file of a second user of the users is storable therein only by the second user, the receiving locker being configured, when opened, to provide to the first user a sender user reference relating to the storage of the third file and to a sender user defined security requirement.

Claim 3 (Previously presented): The method as recited in claim 2 wherein the certificate includes a public key.

Claim 4 (Previously presented): The method as recited in claim 2 further comprising providing a public key to the first user.

Claim 5 (Previously presented): The method as recited in claim 2 wherein the providing the user certificate and the secret key to the first user is performed by providing the user certificate and the secret key on a smart card.

Claim 6 (Previously presented): The method as recited in claim 2 wherein the at least one further security requirement includes at least one of a biometric system requirement, a geographic positioning requirement, a time restriction, a network requirement, and a computer data requirement.

Claim 7 (Previously presented): The method as recited in claim 6 wherein the at least one further security requirement includes a time dependency.

Claim 8 (Previously presented): The method as recited in claim 2 wherein the at least one further security requirement is a requirement of at least one of the operator of the server, the first user, and a sender of the third file.

Claim 9 (Previously presented): The method as recited in claim 2 wherein the provisioning locker has a name associated therewith.

Claim 10 (Previously presented): The method as recited in claim 2 wherein the provisioning locker includes a user locker for the another user.

Claim 11 (Previously presented): The method as recited in claim 2 wherein the receiving locker has a name associated with a sender of the third file.

Claim 12 (Previously presented): The method as recited in claim 2 wherein the receiving locker includes a user locker for the sender user.

Claim 13 (Currently amended): The method as recited in claim 2 wherein the first user and the second user are each registered with the server, and further including the steps of:

setting up a second personal main folder on the server for the second user, the second main folder having a respective first special file including a respective first security requirement defined for the respective main folder and respective management information so as to provide a respective locker,

configuring each respective main folder to have respective further folders set up therein, the respective further folders each having a respective function and each having a

respective second file including a respective second security requirement defined for the respective further folders and including the respective management information, each of the further folders acting as a respective functional locker,

displaying each functional locker only if a respective security-relevant requirement is met, so as to provide a respective locker system having a virtual character, each functional locker providing a respective function of at least one of:

a respective personal locker, respective first files being storable in the respective personal locker only by the respective user and displayable only to the respective user;

a respective provisioning locker, wherein a respective first reference to a respective second file for a different ~~other~~ user being storable by the respective user therein;

a respective receiving locker for a respective third file available to a respective sender user of the users, the respective receiving locker being configured, when opened, to provide to the respective user a respective sender user reference relating to the storage of the respective third file and to a respective sender user defined security requirement; and

a respective public locker configured to store, by the first user, the first reference to the second file when the first reference is stored in the provisioning locker, if access to the first reference is offered to a plurality of different ~~other~~ users.

Claim 14 (Previously presented): The method as recited in claim 2 further including the steps of:

storing a fourth file in the functional locker only if the second security requirement is met;

generating a random number from data of the fourth file so as to provide an access key;

encrypting the data using the access key;

subsequently encrypting the access key with a public key and then destroying the access key so that the access key, for accessing the stored file, can only be recovered using the secret key;

receiving, at the server, the encrypted data, a fourth management information of the fourth file, and the encrypted access key;

encrypting, by the server, the transmitted encrypted data a second time;

generating a unique file identifier for the fourth file;

storing the fourth file in a system locker using the unique file identifier; and

storing a fourth reference to the fourth file in the functional locker, the fourth reference including the unique file identifier, the encrypted access key, and the fourth management information.

Claim 15 (Previously presented): The method as recited in claim 14 wherein the functional locker is the provisioning locker including a user file for the other user, and further including the steps of:

enabling the stored fourth file to be forwarded by the first user to the other user only if the first user decrypts the encrypted access key with the secret key and re-encrypts the decrypted access key with a second public key of the other user, and

storing the re-encrypted access key, the file unique identifier and the fourth management information, as the fourth reference to the file into the user locker.

Claim 16 (Previously presented): The method as recited in claim 14, wherein the second management information includes a management requirement, and wherein the storing the fourth file is performed only if the management requirement is met.